APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/994,878	12/19/1997	MICHAEL A. EPSTEIN	PHA-23.313	7153

7590   04/07/2003

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN, NY 10591

EXAMINER
SONG, HOSUK

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Paper No. 28

Application Number: 08/994,878
Filing Date: December 19, 1997
Appellant(s): EPSTEIN, MICHAEL A.

MAILED

APR 0 7 2003

Technology Center 2100

Michael Epstein
<u>For Appellant</u>

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/10/03.

(1)   *Real Party in Interest*

A statement identifying the real party in interest is contained in the brief.

(2)   *Related Appeals and Interferences*

A statement identifying the related appeals and interferences which will directly

affect or be directly affected by or have a bearing on the decision in the pending appeal

is contained in the brief.

(3)   *Status of Claims*

The statement of the status of the claims contained in the brief is correct.

(4)   *Status of Amendments After Final*

The appellant's statement of the status of amendments after final rejection

contained in the brief is correct.

(5)   *Summary of Invention*

The summary of invention contained in the brief is correct.

(6)   *Issues*

The appellant's statement of the issues in the brief is correct.

(7)   *Grouping of Claims*

The rejection of claims 5-8 stand or fall together because appellant's brief does

not include a statement that this grouping of claims does not stand or fall together and

reasons in support thereof. See 37 CFR 1.192(c)(7).

(8)   *Claims Appealed*

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   *Prior Art of Record*

| 5919257 | TROSTLE | 7-1999 |
| 5903882 | ASAY ET AL. | 5-1999 |

SCHNEIER, BRUCE "Applied Cryptography"Second Edition (10-1996), page 174

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5,7 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Trostle (US 5,919,257) in view of Asay et al.(US 5,903,882).

In claim 5, Trostle, teaches user transmitting ID over the network in (col.5,lines

50-51). Trostle discloses reading from a storage data corresponding to the user having

the received ID, which data comprises the user's private key encrypted using a key

determined from identifying information of the user and sending via network the

encrypted private key,whereby the encrypted key can be received and decrypted at the

location of the user's identifying information in (col.5,lines 51-57). Trostle does not

discloses destroying any non-volatile record of the private key at the location of the

user. Asay disclose in (col.30,lines 55-57 and col.55,lines 38-43) where after

application is signed by a private key, private key is destroyed at the user's site. It

would have been obvious to person of ordinary skill in the art at the time invention was

made to destroy a private key at the user's site taught in Asay with a public key system

disclosed in Trostle in order to assure the user that private key is no longer available for

access if attempted by the hackers and since private key is discarded at the user's site,

the user has total control of its key rather than key handled at the remote site where it

can be viable for attacks.

In Claim 7, the examiner takes Official notice that hashing a document is

well known in the art. The most common cryptographic uses of hash functions are with

digital signatures and for data security. One of ordinary skill in the art would be

motivated to use hash function in order to save both time and space.

Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Trostle in view of Schneier and further in view of Asay.

In claims 6,8, Trostle discloses all the limitations above. However, Trostle does

not discloses passphrase scheme. Schneier discloses passphrase scheme in (page

174,passphrase section). It would have been obvious to one of ordinary skill in the art

at the time the invention was made to use passphrase taught in Schneier for password

of Trostle so that user can remember phrases easier than random character

sequences. Passphrase provides greater security through increased entropy than a

short password. Trostle/Schneier does not disclose processing user's approval of the

document. Asay's patent disclose digitally signing a user's approval document using a

private key. It would have been obvious to person of ordinary skill in the art at the time

invention was made to have approval/validation process done by the use as taught in

Asay with validation process disclosed in Trostle so that if the system is idle or left

unattended by the user any intruders or hackers can compromise the system. Manual

validation process such as digital signing of the document done by the user assures

security. The examiner takes Official notice that hashing a document is well known in

the art. The most common cryptographic uses of hash functions are with digital

signatures and for data security. One of ordinary skill in the art would be motivated to

use hash function in order to save both time and space.

(11)   *Response to Argument*

Appellant on pages 4-5 of the brief argues that Asay teaches the destruction of a

private, and subsequent reconstruction of the key in order to form the user's private key

and citing "In Asay, a clear copy of the key is destroyed, but an encrypted copy of the

key is made and stored" and that " Asay specifically teaches making a non-volatile

record of the user's private key, and does not teach destroying this non-volatile record

of this private key".

In response: attention is directed to claim 5, which recites "destroying *or*

avoiding making any non-volatile record of the private key at the location of the user".

Even though Asay patent teaches storing the corresponding private key in the

subscriber's system. Asay specifically discloses destroying the private key in

subscriber's system in (col.30,lines 55-57). As Appellant recites limitations in the
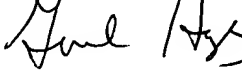
alternative, the broadest interpretation of the claim is that it covers either not both.
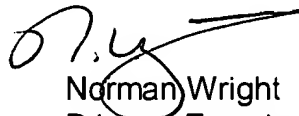
Further, applicant is broadly claiming destroying a private key at the user's site

only but does not claim complete deletion/erase/destroy of all key copy in user's

system. As the claim language is broad enough to read on destruction of just one copy,

Asay meets the claim and currently recited.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Hosuk Song
April 3, 2003

Conferees
Gail Hayes
Supervisory Patent Examiner
Art Unit 2131

Norman Wright
Primary Examiner
Art Unit 2134

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN, NY 10591